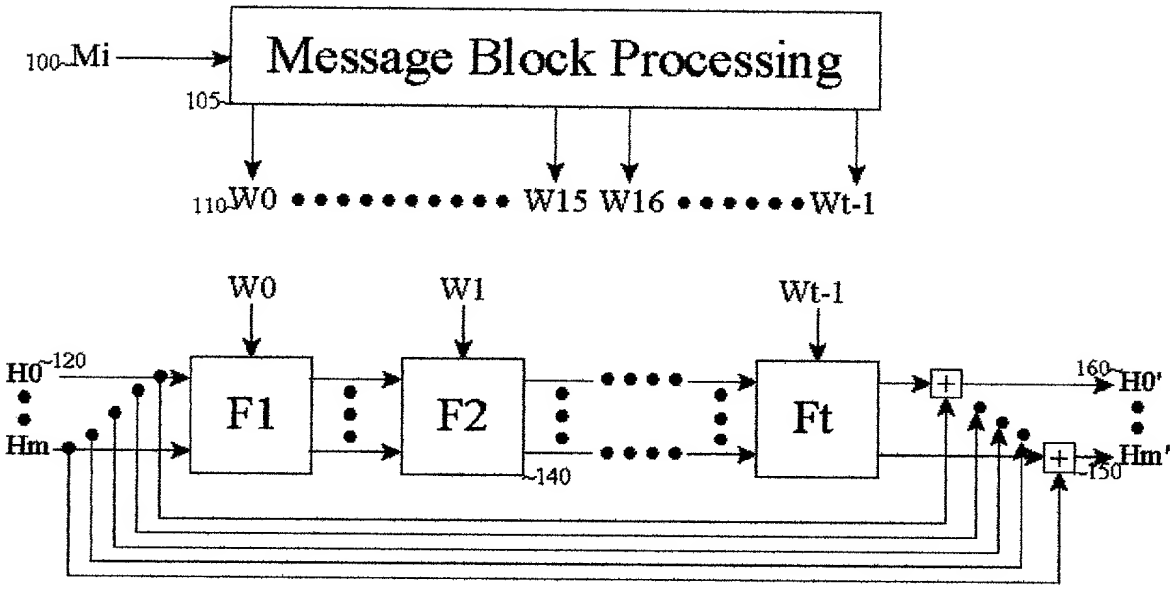

100 Mi
Message Block Processing
105
110 W0 W15 W16 Wt-1
W0
W1
Wt-1
H0
120
Hm
F1
F2
Ft
140
160
H0'
Hm'
150

Fig. 1

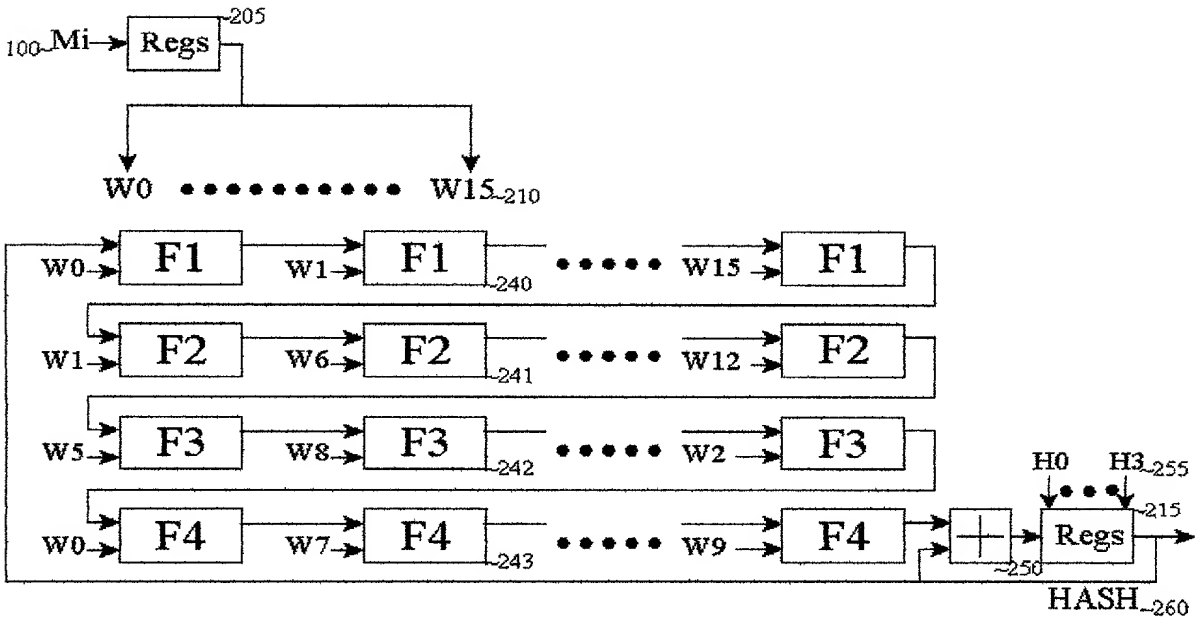

100 Mi
Regs
205
W0
W15
210
F1
F2
F3
F4
240
241
242
243
H0
H3
255
215
250
Regs
HASH
260

Fig. 2

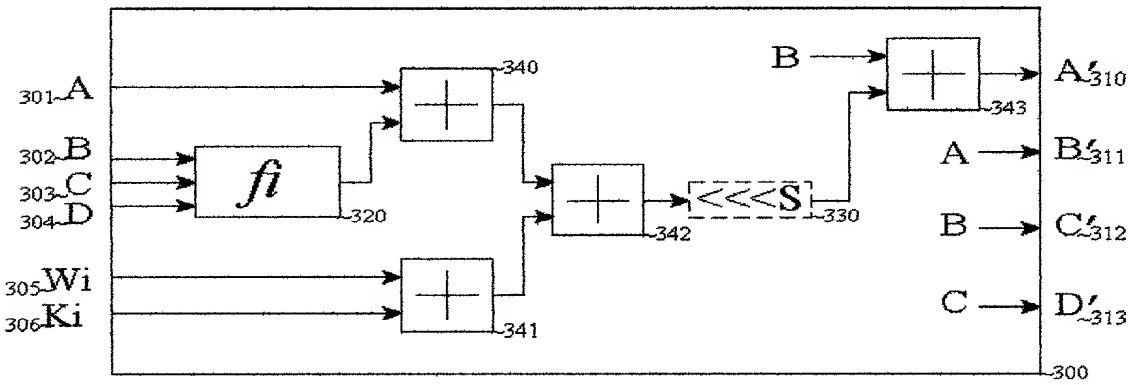

301 A
302 B
303 C
304 D
305 Wi
306 Ki
fi
320
340
341
342
<<<S
330
343
A'
310
B'
311
C'
312
D'
313
300

Fig. 3

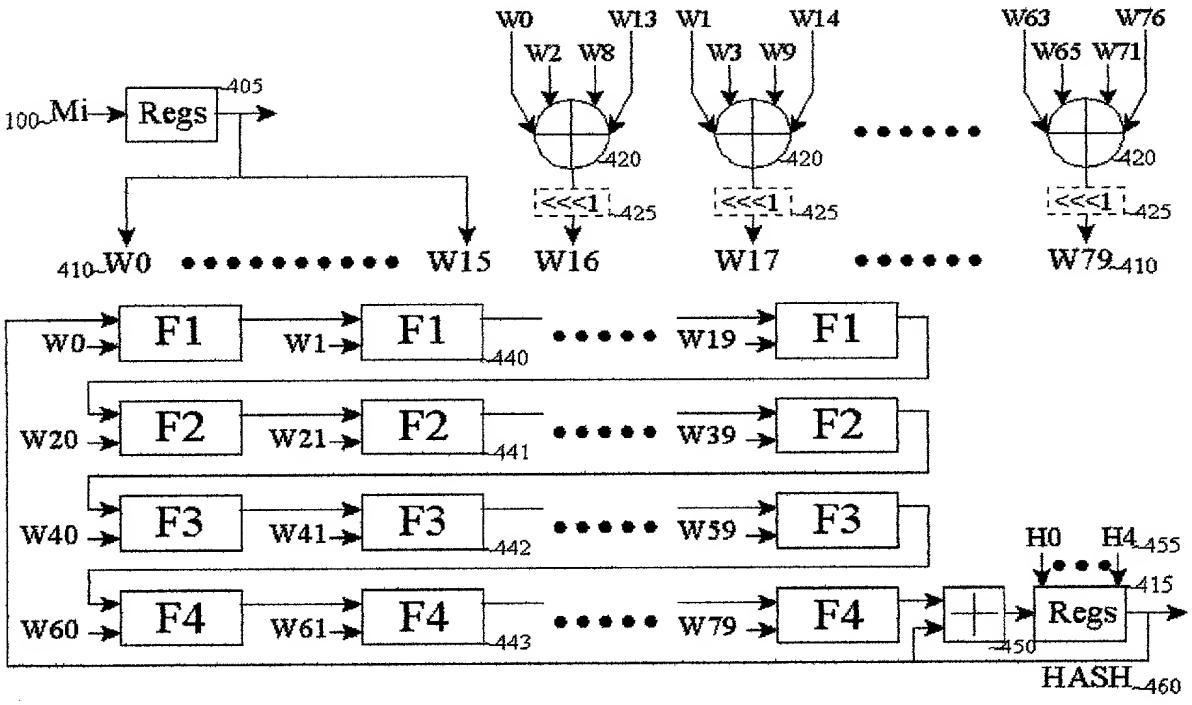

100 Mi
Regs
405
W0
W13
W1
W14
W63
W76
W2
W8
W3
W9
W65
W71
420
<<<1
425
410 W0
W15
W16
W17
W79
410
F1
F2
F3
F4
W0
W1
W19
W20
W21
W39
W40
W41
W59
W60
W61
W79
440
441
442
443
H0
H4
455
415
Regs
450
HASH
460

Fig. 4

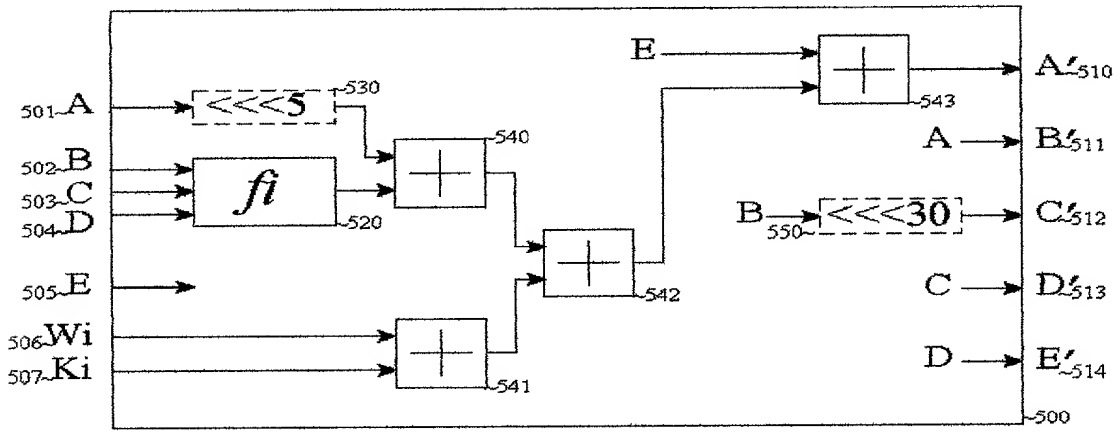

501 A
502 B
503 C
504 D
505 E
506 Wi
507 Ki
<<<5
530
fi
520
540
541
542
543
E
A'
510
A
B'
511
B
<<<30
550
C'
512
C
D'
513
D
E'
514
500

Fig. 5

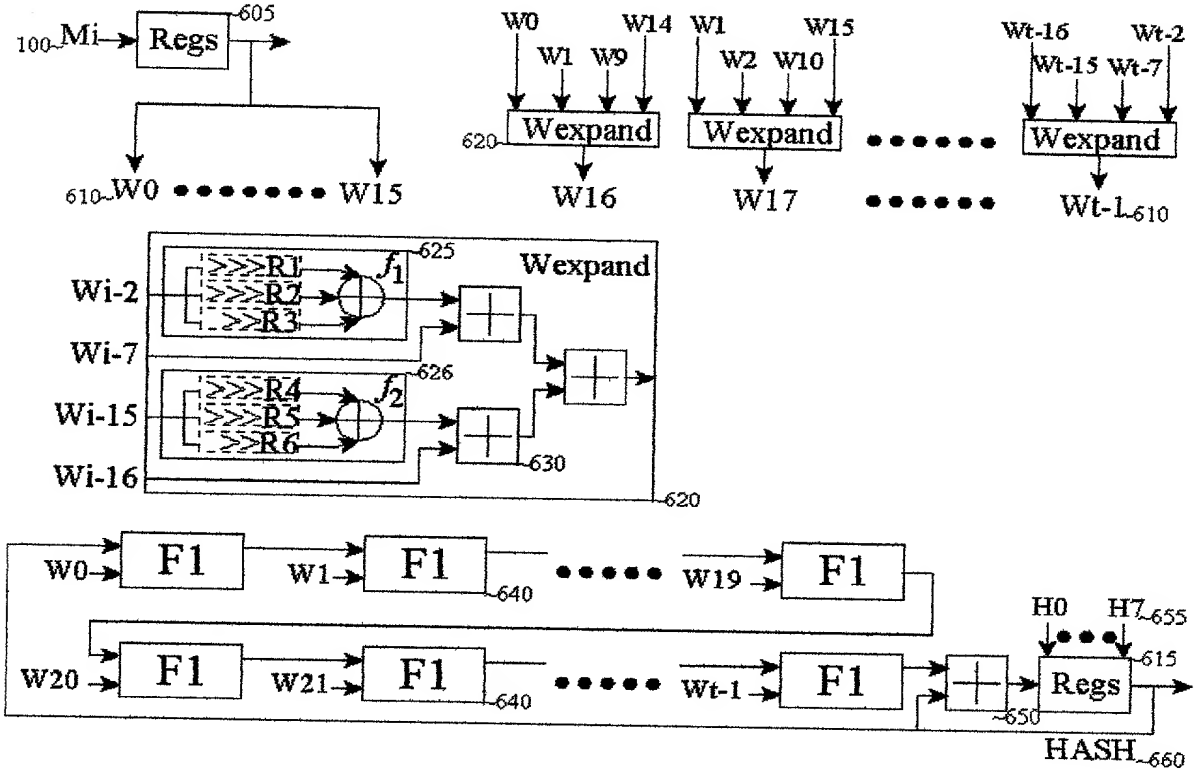

100 Mi
Regs
605
610 W0 W15
W0 W14 W1 W15
W1 W9 W2 W10
Wt-16 Wt-2
Wt-15 Wt-7
620 Wexpand
W16
W17
Wt-1 610
Wi-2
Wi-7
Wi-15
Wi-16
R1 R2 R3
R4 R5 R6
f_1
f_2
625
626
630
620
W0 F1 W1 F1 640 W19 F1
W20 F1 W21 F1 640 Wt-1 F1
H0 H7 655
615
650
HASH 660

Fig. 6

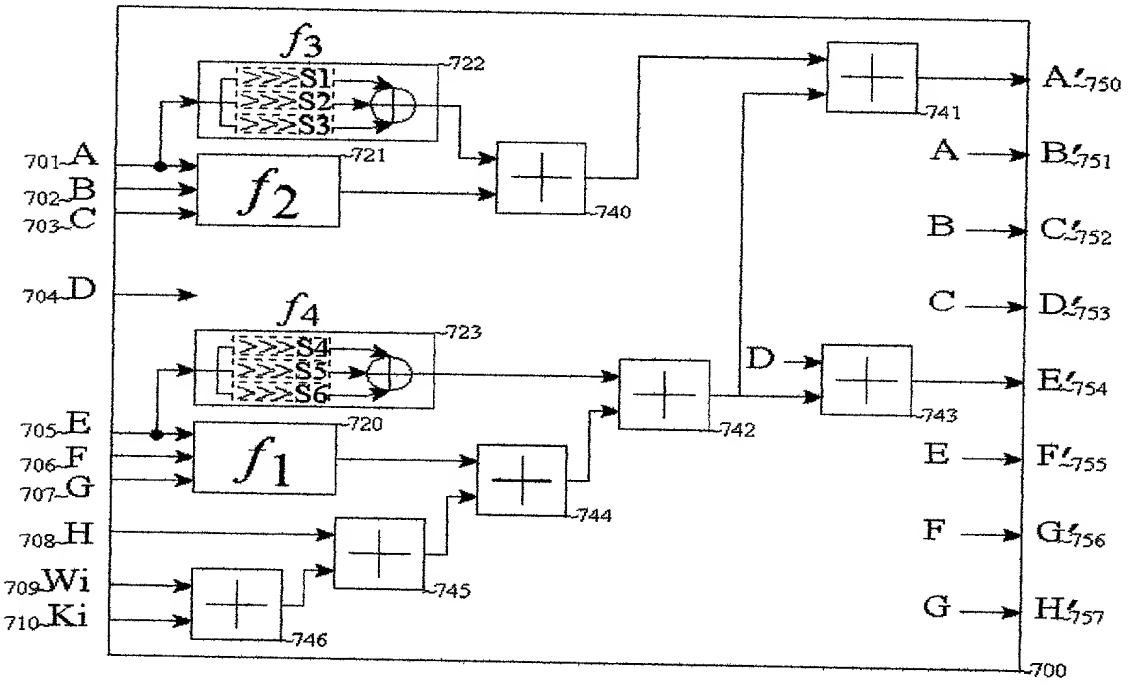

f_3
S1 S2 S3
722
701 A
702 B
703 C
f_2
721
740
741
A′ 750
A 751 B′
B 752 C′
704 D
f_4
S4 S5 S6
723
C 753 D′
D
743
742
E 754 E′
705 E
706 F
707 G
f_1
720
744
E 755 F′
708 H
745
F 756 G′
709 Wi
710 Ki
746
G 757 H′
700

Fig. 7

h1(X, Y, Z) = (X AND Y) OR (~X AND Z)

h2(X, Y, Z) = X XOR Y XOR Z

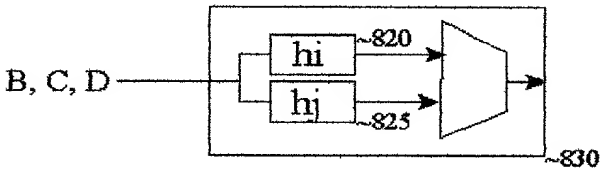
h3(X, Y, Z) = (X AND Y) OR (X AND Z) OR (Y AND Z)

h4(X, Y, Z) = Y XOR (~Z AND X)

(a)

Group	1	2	3	4	5	6	7	8
Rounds	1-16	17-20	21-32	33-40	41-48	49-60	61-64	65-80
MD5	h1	h1'	h1'	h2	h2	h4	h4	
SHA-1	h1	h1	h2	h2	h3	h3	h2	h2

(b)



(c)

Fig. 8

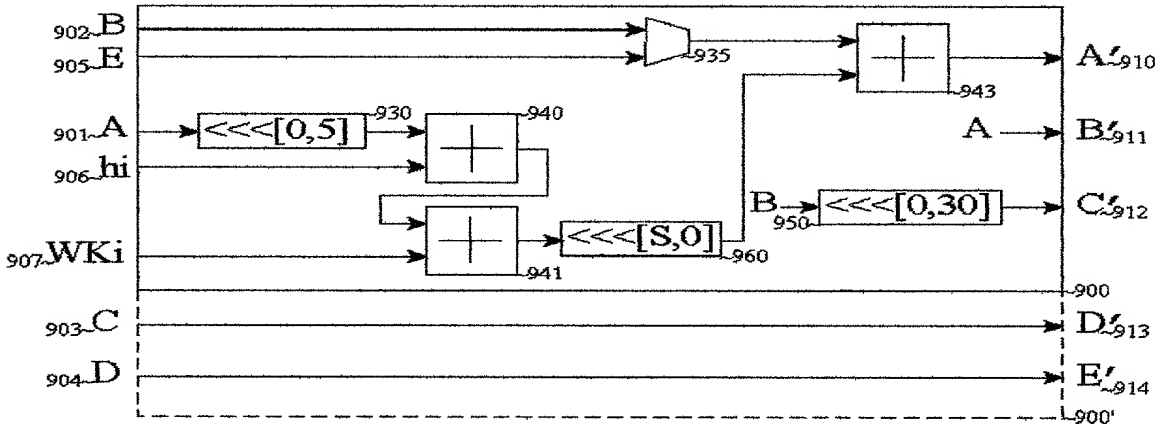


Fig. 9

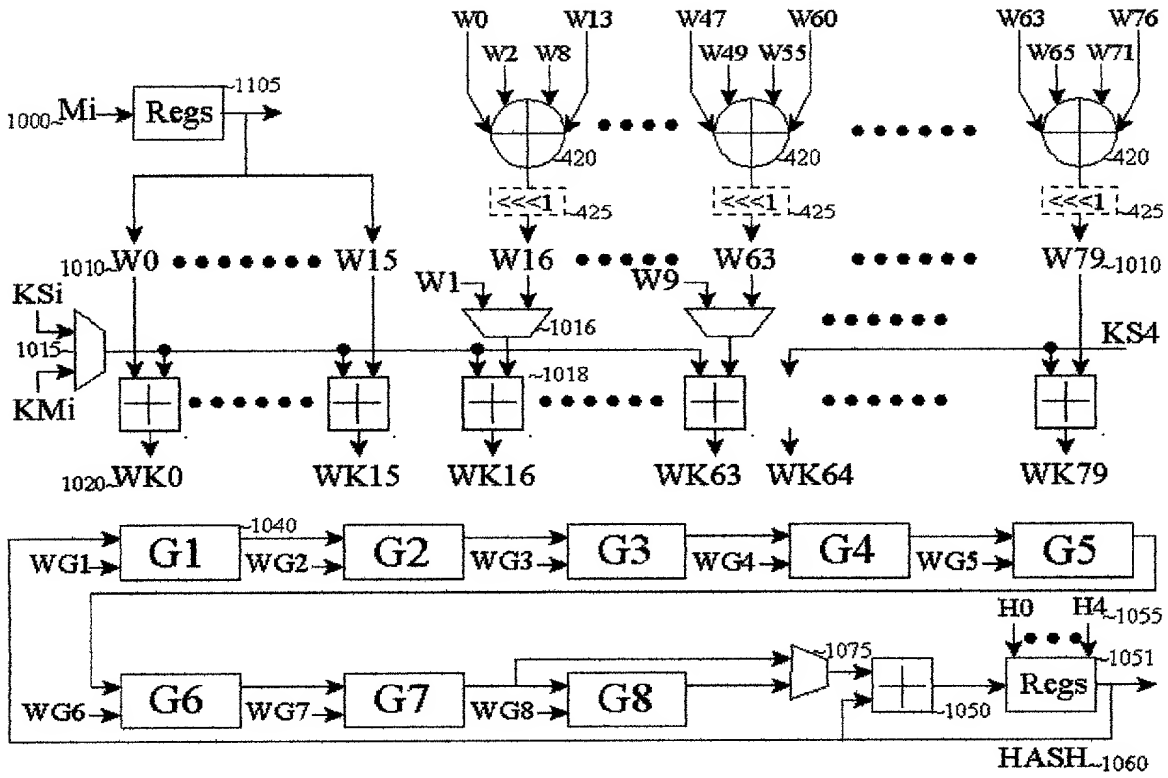

W0
W13
W47
W60
W63
W76
W2
W8
W49
W55
W65
W71
1000
Mi
Regs
1105
420
<<<1
425
1010
W0
W15
W16
W63
W79
KSi
1015
KMi
W1
W9
1016
1018
KS4
1020
WK0
WK15
WK16
WK63
WK64
WK79
1040
WG1
G1
WG2
G2
WG3
G3
WG4
G4
WG5
G5
H0
H4
1055
1075
1051
WG6
G6
WG7
G7
WG8
G8
1050
Regs
HASH
1060

Fig. 10